Number	Category Name	Category Description	HL7 BH Conformance Profile Classification CM = Care Management
	Functional Requirements		
F01	***Identify and maintain a client record***	Key identifying information is stored and linked to the client record. Both static and dynamic data elements will be maintained. A look up function uses this information to uniquely identify the client.	DC \ Care Management
F02	***Manage client demographics***	Contact information including addresses and phone numbers, as well as key demographic information such as date of birth, gender, and other information is stored and maintained for reporting purposes and for the provision of care.	DC \ Care Management
F03	***Manage diagnosis list***	Create and maintain client specific diagnoses.	DC \ Care Management
F04	***Manage medication list***	Create and maintain client specific medication lists- Please see DC.1.7.1 for medication ordering as there is some overlap.	DC \ Care Management
F05	***Manage allergy and adverse reaction list***	Create and maintain client specific allergy and adverse reaction lists.	DC \ Care Management
F06	***Manage client history***	Capture, review, and manage services/treatment, hospitalization information, other information pertient to clients care.	DC \ Care Management
F07	***Summarize health record***		DC \ Care Management
F08	***Manage clinical documents and notes***	Create, correct, authenticate, and close, as needed, transcribed or directly entered clinical documentation.	DC \ Care Management
F09	***Capture external clinical documents***	Incorporate clinical documentation from external sources.	DC \ Care Management
F10	***Generate and record client specific instructions***	Generate and record client specific instructions as clinically indicated.	DC \ Care Management

F11	***Order medication***	Create prescriptions or other medication orders with detail adequate for correct filling and administration.	DC \ Care Management
F12	***Order diagnostic tests***	Submit diagnostic test orders based on input from specific care providers.	DC \ Care Management
F13	***Manage order sets***	Provide order sets based on provider input or system prompt, medication suggestions, drug recall updates.	DC \ Care Management
F14	***Manage results***	Route, manage, and present current and historical test results to appropriate clinical personnel for review, with the ability to filter and compare results.	DC \ Care Management
F15	***Manage consents and authorizations***	Create, maintain, and verify client treatment decisions in the form of consents and authorizations when required.	DC \ Care Management
F16	***Support for standard care plans, guidelines, protocols***	Support the use of appropriate standard care plans, guidelines, and/or protocols for the management of specific conditions.	DC \ Care Management
F17	***Capture variances from standard care plans, guidelines, protocols***	Identify variances from client-specific and standard care plans, guidelines, and protocols.	DC \ Care Management
F18	***Support for drug interaction***	Identify drug interaction warnings at the point of medication ordering	CM \ Clinical Decision Support

F19	***Support for medication or immunization administration or supply***	To reduce medication errors at the time of administration of a medication, the client is positively identified; checks on the drug, the dose, the route and the time are facilitated. Documentation is a by- product of this checking; administration details and additional client information, such as injection site, vital signs, and pain assessments, are captured. In addition, access to online drug monograph information allows providers to check details about a drug and enhances client education.	CM \ Clinical Decision Support
F20	***Support for non-medication ordering***	Referrals, care management	CM \ Clinical Decision Support
F21	***Present alerts for disease management, preventive services and wellness***	At the point of clinical decision making, identify client specific suggestions / reminders, screening tests / exams, and other preventive services in support of disease management, routine preventive and wellness client care standards.	CM \ Clinical Decision Support
F22	***Notifications and reminders for disease management, preventive services and wellness***	Between healthcare service/treatments, notify the client and/or appropriate provider of those preventive services, tests, or behavioral actions that are due or overdue.	CM \ Clinical Decision Support
F23	***Clinical task assignment and routing***	Assignment, delegation and/or transmission of tasks to the appropriate parties.	CM \ Operations Management & Communication

F24	***Inter-provider communication***	Support secure electronic communication (inbound and outbound) between providers in the same practice to trigger or respond to pertinent actions in the care process (including referral), document non-electronic communication (such as phone calls, correspondence or other service/treatments) and generate paper message artifacts where appropriate.	CM \ Operations Management & Communication
F25	***Pharmacy communication***	Provide features to enable secure and reliable communication of information electronically between practitioners and pharmacies or between practitioner and intended recipient of pharmacy orders.	CM \ Operations Management & Communication
F26	***Provider demographics***	Provide a current directory of practitioners that, in addition to demographic information, contains data needed to determine levels of access required by the EHR security and to support the delivery of mental health services.	SS \ Clinical Support
F27	***Scheduling***	Support interactions with other systems, applications, and modules to provide the necessary data to a scheduling system for optimal efficiency in the scheduling of client care, for either the client or a resource/device.	SS \ Clinical Support
F28	***Report Generation***	Provide report generation features for the generation of standard and ad hoc reports	SS \ Measurement, Analysis, Research & Reports
F29	***Health record output***	Allow users to define the records and/or reports that are considered the formal health record for disclosure purposes, and provide a mechanism for both chronological and specified record element output.	SS \ Measurement, Analysis, Research & Reports

F30	***Service/treatment management***	Manage and document the health care delivered during an service/treatment.	SS \ Administrative & Financial
F31	***Rules-driven financial and administrative coding assistance***	Provide financial and administrative coding assistance based on the structured data available in the service/treatment documentation.	SS \ Administrative & Financial
F32	***Eligibility verification and determination of coverage***		SS \ Administrative & Financial
F33	***Manage Practitioner/Patient relationships***	Identify relationships among providers treating a single client, and provide the ability to manage client lists assigned to a particular provider.	SS \ Administrative & Financial
F34	***Clinical decision support system guidelines updates***	Receive and validate formatted inbound communications to facilitate updating of clinical decision support system guidelines and associated reference material	SS \ Administrative & Financial
F35	***Enforcement of confidentiality***	Enforce the applicable jurisdiction's client privacy rules as they apply to various parts of an EHR-S through the implementation of security mechanisms.	INI \ Security
F36	***Data retention, availability, and destruction***	Retain, ensure availability, and destroy health record information according to organizational standards. This includes: Retaining all EHR-S data and clinical documents for the time period designated by policy or legal requirement; Retaining inbound documents as originally received (unaltered); Ensuring availability of information for the legally prescribed period of time; and Providing the ability to destroy EHR data/records in a systematic way according to policy and after the legally prescribed retention period.	INI \ Health Record Information & Management

F37	***Audit trails***	Provide audit trail capabilities for resource access and usage indicating the author, the modification (where pertinent), and the date and time at which a record was created, modified, viewed, extracted, or removed. Audit trails extend to information exchange and to audit of consent status management (to support DC.1.5.1) and to entity authentication attempts. Audit functionality includes the ability to generate audit reports and to interactively view change history for individual health records or for an EHR-system.	INI \ Health Record Information & Management
F38	***Extraction of health record information***	Manage data extraction in accordance with analysis and reporting requirements. The extracted data may require use of more than one application and it may be pre-processed (for example, by being de-identified) before transmission. Data extractions may be used to exchange data and provide reports for primary and ancillary purposes.	INI \ Health Record Information & Management
F39	***Concurrent Use***	EHR system supports multiple concurrent physicians through application, OS and database.	SS \ Clinical Support
F40	***Mandated Reporting***	Manage data extraction accordance with mandating requirements.	SS \ Measurement, Analysis, Research & Reports
F41	***Administrative A/P E.H.R. Support***		
F42	***Administrative A/R E.H.R. Support***		
F43	***Administrative Workflows E.H.R. Support***		
	Security Requirements		
S01	**Security: Access Control**		
S02	**Security: Authentication**		

S03	**Security: Documentation**		
S04	**Security: Technical Services**		
S05	**Security: Audit Trails**		
S06	**Reliability: Backup/Recovery**		
S07	**Reliability: Documentation**		
S08	**Reliability: Technical Services**		
	Interoperability Requirements		
I01	**Laboratory**		DC \ Care Management
I02	**Imaging**		
I03	**Medications**		
I04	**Clinical Documentation**		
I05	**Chronic Disease Management/ Patient Documentation**		
I06	**Secondary Uses of Clinical Data**		
I07	**Administrative & Financial Data**		

California Department of Mental Health

MHSA - Behavioral Health Functional
Functional Criteria MHSA Evaluation of EHRs

DMH EHR Functional Requirement Category Number	DMH EHR Functional Requirement Criteria Number	Specific Criteria	Discussion / Comments	EHR Road Map 1=Infrastructure 2=Practice Mgmt 3=Clinical Data 4=CPOE 5=Full EHR 6=Full EHR/PHR		Vendor Ratings Availability			
						2006	2007	2008	2009 and beyond
F-35	35.001	The system shall be able to audit the date/time and user of each instance when a client chart is printed by the system.	Does not include screen print and other functions that are external to the programmed functionality of the EHR system.	1		M	M	H	
F-35	35.002	The system shall provide a means to document a client's dispute with information currently in their chart.	This does not imply that the client can document directly in their chart. Some methods include but are not limited to allowing the client a view only access to their record, printing a copy of the record for a client to review. Methods to include the information in the chart could be as a note, a scanned copy of client comments, an addendum to the note or other method not described.	1		L	L	M	H
F-35	35.003	The system shall be able to identify all users who have accessed an individual's chart over a given time period, including date and time of access.	Specific items/sections of information accessed shall be identified, with appropriate audit trail.	1		M	M	H	
F-35	35.004	The system shall be able to identify certain information as confidential and only make that accessible by appropriately authorized users.	This may be implemented by having a "confidential" section of the chart	1		M	M	H	
F-35	35.005	The system shall be able to prevent specified user(s) from accessing a designated client's chart	An example would be preventing access to a VIP or staff member's chart. When access is restricted, the system shall provide a means for appropriately authorized users to "break the glass" for emergency situations. Such overrides shall be audited.	1		M	L	M	H

F-36	36.001	The system shall be able to retain data until otherwise purged, deleted, archived or otherwise deliberately removed.		1		H			
F-36	36.002	The system shall provide a method for archiving health record information.	Archiving is used to mean information stored in a retrievable fashion without defining where or how it is stored.	1		L	M	H	
F-36	36.003	The system shall be able to retrieve information that has been archived.	Retrieval does not imply restoration to current version of the software.	1					
F-36	36.004	The system shall be able to store and retrieve health record data and clinical documents for the legally prescribed timeframes.		1					
F-36	36.005	The system shall be able to retain inbound data or documents (related to health records), as originally received (unaltered, inclusive of the method in which they were received), for the legally prescribed time frames, in accordance with users' scope of practice, organizational policy or jurisdictional law.		1					
F-36	36.006	The system shall be able to retrieve information in a manner conducive to recreating the context in which the information was obtained.		1					
F-36	36.007	The system shall be able to retrieve all the elements included in the definition of a legal health (medical) record.		1					
F-36	36.008	The system shall provide for oversight, review and confirmation of record(s) destruction prior to destroying specific EHR data/records.		1					
F-36	36.009	The system shall be able to destroy EHR data/records so that all traces are unrecoverable, according to policy and legal retention periods.		1					
F-37	37.001	The system shall be able to log outgoing information exchange in an auditable form.	In future, the work group will clarify details of what shall be included in the log, and revise timing of this criterion based on those elements, if required.	1		L	L	H	
F-37	37.002	The system shall be able to log the receipt of documents in an auditable form.		1		L	L	M	H
F-37	37.003	The system shall track and can produce a report of every transaction initiated on the system, identifying the user, location, date, time, function, file accessed, record accessed. There will be sufficient capacity to archive this information for 7 years. Transactions include read, write, execute, and delete. The system will support internal audit and review by the local Privacy Officer.		1					

F-37	37.004	The system shall allow administrators control over which system components will have audit controls in place and what types of audit trails are utilized.	Examples are: tracking record additions, edits, and deletions, but not record lookups.	1					
F-38	38.001	The system shall be able to export (extract) pre-defined set(s) of data out of the system	For example, export of performance measures, ability to query data base, chronic disease management tools.	1		H			
F-38	38.002	The system shall be able to import data into the system	Data import implies receiving discrete data into the EHR in an automated manner as opposed to manual data entry or document scanning. This could be accomplished via a real time or batch interface or a manual data load.	1		M	H		
F-38	38.003	The system shall allow removal of discrete client identifiers.	De-identification is necessary for research purposes, e.g., to identify patterns of disease. External applications can be used to meet this criteria.	1		L	M	H	
F-38	38.004	The system shall be able to specify the intended destination of the extracted information.	The user may indicate to whom they are sending results. The lack of control of information once it leaves the practice is acknowledged.	1		L	L	M	H
F-39	39.001	The system shall allow multiple users to interact concurrently with the EHR application.		1		H			
F-39	39.002	The system shall allow concurrent users to simultaneously view the same EHR administrative and / or financial record data.		1		H			
F-39	39.003	The system shall allow concurrent users to view the same EHR clinical documentation or template.		1		H			
F-39	39.004	The system shall provide protection to maintain the integrity of clinical data during concurrent access.	To prevent users from simultaneously attempting to update a record with resultant loss of data	1		H			
F-39	39.005	The system shall simultaneously trigger alerts to users of each other's presence in the same record, where such access is permitted.	Moved from Admin Workflow 43.044.	1					
F-43	43.013	The system shall support the downloading, uploading and security of data to and from mobile devices such as laptops, tablet computers, and personal digital assistants, to support mobile workers.		1					
F-43	43.038	The system shall be scalable to meet current and future user access and data storage needs.		1					

F-43	**43.039**	The system shall incorporate a consistent user interface (UI) for data entry. The UI design should independent of the proposed hardware configuration.		**1**					
F-43	**43.040**	The system shall support a variety of data input modalities, including: Voice recognition, Touch screen, Light pen, Mouse, Keyboard		**1**					
F-43	**43.041**	The system shall support remote system monitoring technology.		**1**					
F-43	**43.042**	The system shall incorporate extensive, secure capabilities that link staff and clinicians from remote locations to the central site.		**1**					
F-43	**43.047**	The system shall support industry standard locking mechanisms to prevent multiple users from simultaneously accessing/updating patient data as appropriate.		**1**					
F-43	**43.048**	The system shall support and implement redundancy/fault tolerance for 100% availability.		**1**					
F-43	**43.049**	The system shall Web-based with appropriate security measures to meet HIPAA compliance requirements.		**1**					
F-43	**43.050**	The system shall efficiently manage both structured and unstructured health record information during manual and electronic, retrieval, update, reporting, and tracking processes.	Management of actions involving complete or partial records is included.	**1**					
F-43	**43.051**	The system shall support efficient linkage of all associations between structured and unstructured health record information.	Includes structured to structured, unstructured to unstructured, and structured to unstructured data associations.	**1**					
S-01	**1.001**	The system shall enforce the most restrictive set of rights/privileges or accesses needed by users/groups (e.g. System Administration, Clerical, Nurse, Doctor, etc.), or processes acting on behalf of users, for the performance of specified tasks.		**1**		X			X
S-01	**1.002**	The system shall provide the ability for authorized administrators to assign restrictions or privileges to users/groups.		**1**		X			X

S-01	**1.003**	The system must be able to associate permissions with a user using one or more of the following access controls: 1) user-based (access rights assigned to each user); 2) role-based (users are grouped and access rights assigned to these groups); or 3) context-based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, workstation-location, emergency-mode, etc.)		**1**		X			X
S-01	**1.004**	The system shall support removal of a user's privileges without deleting the user from the system. The purpose of the criteria is to provide the ability to remove a user's privileges, but maintain a history of the user in the system.		**1**			X		
S-01	**1.013**	The system shall provide the ability to create sets of access control permissions granted to users (both human and other applications).		**1**					
S-01	**1.014**	The system shall authorize users to access the applications based on the following: User identity, User role, User work assignment, User location, Client's present condition, Context.		**1**					
S-01	**1.015**	The system shall allow the system administrator to: Add authorized users, Delete (or inactivate) authorized users, Modify a user's current access profile.		**1**					
S-01	**1.016**	The system shall provide the ability to define user access rules.		**1**					
S-01	**1.017**	The system shall enforce the access rules for all EHR resources, based on the application's physical/logical configuration.		**1**					
S-01	**1.018**	The system shall provide the ability to define user access to the application's functions.		**1**					
S-01	**1.019**	The system shall require passwords be changed at a user-defined time interval.		**1**					

S-01	**1.020**	The system shall provide automatic notifications to users upon successful access to the application that the current password is due to expire.		**1**					
S-01	**1.021**	The system shall be able to set the number of days prior to the password expiration date; the system is to display the notification.		**1**					
S-01	**1.022**	The system shall prohibit access to the application by users entering expired passwords.		**1**					
S-01	**1.023**	The system shall provide the ability to automatically log users out of the application after a user-defined number of seconds/minutes of inactivity.		**1**					
S-01	**1.024**	The system shall comply with all appropriate California State and federal legislation Department of Mental Health rules regarding patient confidentiality and privacy.		**1**					
S-01	**1.025**	The system shall maintain varying levels of confidentiality in accordance with users' scope of practice, organizational policy or jurisdictional law.		**1**					
S-01	**1.026**	The system shall allow certain role clinicians to mark a cleint's specific information as blinded, prohibiting access to all other users. Note: The standards in this area are still evolving.	Was 7.001 but Category 7: Security Access Control was consolidated into Category 1: Security Access Control	**1**				X	
S-01	**1.027**	The system shall support access to blinded information to a treating clinician, when the blinded information is necessary for managing an emergency condition. Note: This is commonly known as a "break the glass" function. This does not provide increased access rights for the user.	Was 7.002 but Category 7: Security Access Control was consolidated into Category 1: Security Access Control	**1**				X	
S-01	**1.028**	The "break the glass" function must be capable of requiring the clinician requesting access to blinded information to document and record the reason(s) for requesting access.	Was 7.003 but Category 7: Security Access Control was consolidated into Category 1: Security Access Control	**1**				X	
S-02	**2.001**	The system shall authenticate the user before any access to Protected Resources (e.g. PHI) is allowed, including when not connected to a network e.g. mobile devices.		**1**		X			X

S-02	**2.002**	When passwords are used, the system shall support password strength rules that allow for minimum number of characters, and inclusion of alpha-numeric complexity.		**1**		X			X
S-02	**2.003**	The system upon detection of inactivity of an interactive session shall prevent further viewing and access to the system by that session by terminating the session, or by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures. The inactivity timeout shall be configurable.		**1**		X			X
S-02	**2.004**	The system shall enforce a limit of (configurable) consecutive invalid access attempts by a user. The system shall protect against further, possibly malicious, user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm).		**1**		X			X

S-02	**2.005**	When passwords are used, the system shall provide an administrative function that resets passwords.		**1**		X			X
S-02	**2.006**	When passwords are used, user accounts that have been reset by an administrator shall require the user to change the password at next successful logon.		**1**			X		
S-02	**2.007**	The system shall provide only limited feedback information to the user during the authentication.		**1**		X			X
S-02	**2.008**	The system shall support case-insensitive usernames that contain typeable alpha-numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).		**1**		X			X
S-02	**2.009**	When passwords are used, the system shall allow an authenticated user to change their password consistent with password strength rules (S13).		**1**		X			X
S-02	**2.010**	When passwords are used, the system shall support case-sensitive passwords that contain typeable alpha-numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).		**1**		X			X
S-02	**2.011**	When passwords are used, the system shall not store passwords in plain text.		**1**		X			X
S-02	**2.012**	When passwords are used, the system shall prevent the reuse of passwords previously used within a specific (configurable) timeframe (i.e., within the last X days, etc. - e.g. "last 180 days"), or shall prevent the reuse of a certain (configurable) number of the most recently used passwords (e.g. "last 5 passwords").		**1**			X		
S-02	**2.013**	The system shall authenticate all users (both human and other applications) attempting to access the application.		**1**					
S-02	**2.014**	The system shall provide any of the following types of authentication: Username/password, Digital certificate, Secure token, Biometrics		**1**					
S-02	**2.015**	The system shall provide the ability to implement Chain of Trust agreements.		**1**					
S-02	**2.016**	The system shall support two-factor authentication in alignment with NIST 800-63 Level 3 Authentication. Note: The standards in this area are still evolving.	Was 5.001 but Category 5: Security Authentication was consolidated into Category 2: Security Authentication	**1**					

S-02	**2.017**	When passwords are used, the system shall not transport passwords in plain text.	Was 4.002. Moved to Security Authentication 2.017	**1**		X			X
S-02	**2.018**	When passwords are used, the system shall not display passwords while being entered.	Was 4.003. Moved to Security Authentication 2.018	**1**		X			X
S-03	**3.001**	The system shall include documentation available to the customer that provides guidelines for configuration and use of the EHR security controls necessary to support secure and reliable operation of the system, including but not limited to: creation, modification, and deactivation of user accounts, management of roles, reset of passwords, configuration of password constraints, and audit logs.		**1**		X			X
S-04	**4.001**	The system shall support protection of confidentiality of all Protected Health Information (PHI) delivered over the Internet or other known open networks via encryption using triple-DES (3DES) or the Advanced Encryption Standard (AES) and an open protocol such as TLS, SSL, IPSec, XML encryptions, or S/MIME or their successors.		**1**		X			X
S-04	**4.004**	For systems that provide access to PHI through a web browser interface (i.e. HTML over HTTP) shall include the capability to encrypt the data communicated over the network via SSL (HTML over HTTPS). Note: Web browser interfaces are often used beyond the perimeter of the protected enterprise network		**1**		X			X
S-04	**4.005**	The system shall support protection of integrity of all Protected Health Information (PHI) delivered over the Internet or other known open networks via SHA1 hashing and an open protocol such as TLS, SSL, IPSec, XML digital signature, or S/MIME or their successors.		**1**		X			X
S-04	**4.006**	The system shall support ensuring the authenticity of remote nodes (mutual node authentication) when communicating Protected Health Information (PHI) over the Internet or other known open networks using an open protocol (e.g. TLS, SSL, IPSec, XML sig, S/MIME).		**1**		X			X

S-04	**4.007**	The system, when storing PHI on any physical media intended to be portable/removable (e.g. thumb-drives, CD-ROM, PDA), shall support use of a standards based encrypted format using triple-DES (3DES), and the Advanced Encryption Standard (AES).		**1**					
S-04	**4.008**	The system shall have security measures to project data being transmitted via wireless networks, including data communications with portable devices.		**1**					
S-04	**4.009**	The system shall provide the ability to obfuscate (intentionally make difficult to read) data.		**1**					
S-04	**4.010**	The system shall encrypt and de-encrypt data that is received and/or transmitted over a non-secure network.		**1**					
S-04	**4.011**	The system shall support standard data encryption protocols.		**1**					
S-04	**4.012**	The system shall route data only to/from known, registered, and authenticated applications using secure networks.		**1**					
S-04	**4.013**	The system shall provide the ability to store a user identifier with data other than the user who entered that data.		**1**					
S-04	**4.014**	The system shall support the storage of any Protected Health Information (PHI) data on any associated mobile device(s) such as PDAs, smartphones, etc. in an encrypted format, using triple-DES (3DES), the Advanced Encryption Standard (AES), or their successors.	Was 6.001 but Category 5: Security Technical Services was consolidated into Category 4: Security Technical Services	**1**					
S-04	**4.015**	The system, prior to a user login, shall display a (configurable) notice warning (e.g. "The system should only be accessed by authorized users").	Was 6.002 but Category 5: Security Technical Services was consolidated into Category 4: Security Technical Services	**1**					
S-04	**4.016**	The system shall be able to support time synchronization using NTP/SNTP, and use this synchronized time in all security records of time.	Moved from Security Access Control: 1.008	**1**		X			X
S-04	**4.017**	The system shall have the ability to format for export recorded time stamps using UTC based on ISO 8601. Example: "1994-11-05T08:15:30-05:00" corresponds to November 5, 1994, 8:15:30 am, US Eastern Standard Time.	Moved from Security Access Control: 1.009	**1**			X		
S-05	**5.001**	The system shall support logging to a common audit engine using the schema and transports specified in the Audit Log specification of IHE Audit Trails and Node Authentication (ATNA) Profile	Category 8: Security Audit was renumbered as Category 5: Security Audit	**1**					
S-05	**5.002**	The system shall maintain an audit log of all failed access attempts.	Category 8: Security Audit was renumbered as Category 5: Security Audit	**1**					

S-05	**5.003**	The system shall date/time stamp: Initial data entry, Data modificaiton, Exchange of data (date/time data is formatted and transmitted from EHR-S to another application), Data deleted or inactivated, Report requested, Query requested	Category 8: Security Audit was renumbered as Category 5: Security Audit	**1**					
S-05	**5.004**	The system shall store the identity of the user for every instance of: Data entry, Data modification, Exchange of data, Data deleted or inactivated, Report requested, Query performed.	Category 8: Security Audit was renumbered as Category 5: Security Audit	**1**					
S-05	**5.005**	The system shall support any of the following types of user identifiers when storing user identity: Password, Digital certificate, Unique entity identifier (e.g., application's IP address[1], sending facility CLIA[2] number, etc.)	Category 8: Security Audit was renumbered as Category 5: Security Audit	**1**					
S-05	**5.006**	The system shall provide an audit trail of new software versions loaded, or changes to the EHR application.	Category 8: Security Audit was renumbered as Category 5: Security Audit	**1**					
S-05	**5.007**	The system shall provide an audit trail of new versions of standard code sets and knowledge bases.	Category 8: Security Audit was renumbered as Category 5: Security Audit	**1**					
S-05	**5.008**	The system shall provide and audit trail of all successful and unsuccessful backups.	Category 8: Security Audit was renumbered as Category 5: Security Audit	**1**					
S-05	**5.009**	The system shall provide an audit trail of all application recoveries from backup media.	Category 8: Security Audit was renumbered as Category 5: Security Audit	**1**					
S-05	**5.010**	The system shall provide an audit trail of any date/time changes if this is a required activity.	Category 8: Security Audit was renumbered as Category 5: Security Audit	**1**					
S-05	**5.011**	The system shall provide an audit trail for all archiving of data.	Category 8: Security Audit was renumbered as Category 5: Security Audit	**1**					
S-05	**5.012**	The system shall provide an audit trail when re-activating an archived client record.	Category 8: Security Audit was renumbered as Category 5: Security Audit	**1**					
S-05	**5.013**	The system shall provide an audit trail of all user/application entries and exits from the EHR application.	Category 8: Security Audit was renumbered as Category 5: Security Audit	**1**					

S-05	**5.014**	The system shall provide an audit trail of all remote access connections including those for system support and maintenance activities.	Category 8: Security Audit was renumbered as Category 5: Security Audit	**1**					
S-05	**5.015**	The system shall be able to detect security-relevant events that it mediates and generate audit records for them. At a minimum the events shall include: start/stop, user login/logout, session timeout, account lockout, cleint record created/viewed/updated/deleted, scheduling, query, order, node-authentication failure, signature created/validated, PHI export (e.g. print), PHI import, and security administration events. Note: The system is only responsible for auditing security events that it mediates. A mediated event is an event that the system has some active role in allowing or causing to happen or has opportunity to detect. The system is not expected to create audit logs entries for security events that it does not mediate.	Moved from Security Access Control: 1.005.	**1**			X		
S-05	**5.016**	The system shall record within each audit record the following information when it is available: (1) date and time of the event; (2) the component of the system (e.g. software component, hardware component) where the event occurred; (3) type of event (including: data description and cleint identifier when relevant); (4) subject identity (e.g. user identity); and (5) the outcome (success or failure) of the event.	Moved from Security Access Control: 1.006	**1**		X			X
S-05	**5.017**	The system shall provide authorized administrators with the capability to read all audit information from the audit records in one of the following two ways: 1) The system shall provide the audit records in a manner suitable for the user to interpret the information. The system shall provide the capability to generate reports based on ranges of system date and time that audit records were collected. 2) The system shall be able to export logs into text format in such a manner as to allow correlation based on time (e.g. UTC synchronization).	Moved from Security Access Control: 1.007	**1**		X			X
S-05	**5.018**	The system shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. The system shall protect the stored audit records from unauthorized deletion. The system shall prevent modifications to the audit records.	Moved from Security Access Control: 1.010	**1**		X			X
S-05	**5.019**	The system shall allow an authorized administrator to enable or disable auditing for groups of related events to properly collect evidence of compliance with implementation-specific policies. Note: In response to a HIPAA-mandated risk analysis and management, there will be a variety of implementation-specific organizational policies and operational limits.	Moved from Security Access Control: 1.012	**1**			X		

S-06	**6.002**	The system restore functionality shall result in a fully operational and secure state. This state shall include the restoration of the application data, security credentials, and log/audit files to their previous state.	Category 9: Reliability Backup and Recovery was renumbered as Category 6.	**1**		X			X
S-06	**6.003**	If the system claims to be available 24x7 then the system shall have ability to run a backup concurrently with the operation of the application.	Category 9: Reliability Backup and Recovery was renumbered as Category 6.	**1**		X			X
S-06	**6.004**	The system's data and program files are capable of being backed up by common third party backup tools.	Category 9: Reliability Backup and Recovery was renumbered as Category 6.	**1**					
S-06	**6.005**	The system shall provide for the purging and storage of data that is no longer needed on a real-time basis by county staff.	Category 9: Reliability Backup and Recovery was renumbered as Category 6.	**1**					
S-06	**6.006**	The system shall provide for: User defined archiving of data (based on service date, date of last activity, or other user-defined characteristics); Printed reports of data being archived; ability to selectively restore archived data; proper control over archiving of data where a patient has an outstanding balance; archiving data to disk, tape or other storage media.	Category 9: Reliability Backup and Recovery was renumbered as Category 6.	**1**					
S-06	**6.007**	The system shall support efficient recovery from an interruption in the power supply both during business hours and after hours when no staff are on-site, or in other situations where user data has been lost or otherwise compromised.	Category 9: Reliability Backup and Recovery was renumbered as Category 6.	**1**					
S-06	**6.008**	The system architecture allows the system to recover from service interruptions with no or minimal loss of data, as well as minimal level of effort to return the system to the pre-interruption state. Methods are in place to ensure that any data initially lost during a system interruption is readily recoverable.	Category 9: Reliability Backup and Recovery was renumbered as Category 6.	**1**					
S-07	**7.001**	The system shall include documentation available to the customer stating whether or not there are known issues or conflicts with security services in at least the following serivce areas: antivirus, intrusion detection, malware eradication, host-based firewall and the resolution of that conflict (e.g. most systems should note that full virus scanning should be done outside of peak usage times and should exclude the databases.).	Category 10: Reliability: Documentation was renumbered as Category 7.	**1**		X			X
S-07	**7.002**	If the system includes hardware, the system shall include documentation that covers the expected physical environment necessary for proper secure and reliable operation of the system including: electrical, HVAC, sterilization, and work area.	Category 10: Reliability: Documentation was renumbered as Category 7.	**1**		X			X

S-07	**7.003**	The system shall include documentation that itemizes the services (e.g. PHP, web services) and network protocols/ports (e.g. HL-7, HTTP, FTP) that are necessary for proper operation and servicing of the system, including justification of the need for that service and protocol. This information may be used by the healthcare facility to properly configure their network defenses (firewalls and routers).	Category 10: Reliability: Documentation was renumbered as Category 7.	**1**		x			X
S-07	**7.004**	The system shall include documentation that describes the steps needed to confirm that the system installation was properly completed and that the system is operational.	Category 10: Reliability: Documentation was renumbered as Category 7.	**1**		X			x
S-07	**7.005**	The system shall include documentation that describes the patch (hot-fix) handling process the vendor will use for EHR, operating system and underlying tools (e.g. a specific web site for notification of new patches, an approved patch list, special instructions for installation, and post-installation test).	Category 10: Reliability: Documentation was renumbered as Category 7.	**1**		X			x
S-07	**7.006**	The system shall include documentation that explains system error or performance messages to users and administrators, with the actions required.	Category 10: Reliability: Documentation was renumbered as Category 7.	**1**		X			X
S-07	**7.007**	The system shall include documentation of product capacities (e.g. number of users, number of transactions per second, number of records, network load, etc.) and the baseline representative configurations assumed for these capacities (e.g. number or type of processors, server/workstation configuration and network capacity, etc).	Category 10: Reliability: Documentation was renumbered as Category 7.	**1**		X			X
S-07	**7.008**	The system shall include documented procedures for product installation, start-up and/or connection.	Category 10: Reliability: Documentation was renumbered as Category 7.	**1**		X			X
S-07	**7.009**	The system shall include documentation of the minimal privileges necessary for each service and protocol necessary to provide EHR functionality and/or serviceability.	Was 12.001. Category 12: Reliability: Documentation was consolidated into Category 7.	**1**		X			X
S-08	**8.001**	The software used to install and update the system, independent of the mode or method of conveyance, shall be certified free of malevolent software ("malware"). Vendor may self-certify compliance with this standard through procedures that make use of commercial malware scanning software.	Category 11: Reliability: Technical Services was renumbered as Category 8.	**1**		X			X
S-08	**8.002**	The system shall be accessible and available for all authorized users 99.5% of the time.	Category 11: Reliability: Technical Services was renumbered as Category 8.	**1**					
S-08	**8.003**	The system shall support response times of 2 seconds or less 90% of the time.	Category 11: Reliability: Technical Services was renumbered as Category 8.	**1**					
S-08	**8.004**	The system shall support sub-second response times 80% of the time.	Category 11: Reliability: Technical Services was renumbered as Category 8.	**1**					
S-08	**8.005**	The system shall support and implement redundancy/fault tolerance for 100% availability.	Category 11: Reliability: Technical Services was renumbered as Category 8.	**1**					
S-08	**8.006**	The system shall be configurable to prevent corruption or loss of data already accepted into the system in the event of a system failure (e.g. integrating with a UPS, etc.).	Was 13.001. Category 13: Reliability: Technical Services was consolicated into Category 8.	**1**		X			X